Application No.:09/940,706
Filing Date: 08/28/2001

Docket No.: JP920010196US1

IN THE CLAIMS

Please amend the claims as set out below:

1. (currently amended) A method for providing secure authentication, the method comprising:

a) sending ~~receiving~~ basic authentication data from a first computer to a second computer, wherein the basic authentication data provides a certificate including a validity status date and a credential, the credential being for permitting a first type of transaction access by the first computer to an application provided by the second computer ~~for a secure transaction between the first computer and a second computer; wherein the receiving is by the second computer~~, wherein ~~the secure transaction is during a certain communication session between the first and second computer, and~~ the basic authentication data has been certified by an accepted certifying authority, and ~~wherein~~ the basic authentication data sent to the second computer includes a public key of the first computer ~~for permitting a first type of access by the first computer to an application provided by the second computer~~;

~~b) storing a copy of the first computer's public key;~~

~~c) requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer;~~

b~~d~~) generating ~~receiving the~~ an additional individual authentication data unit by the ~~second computer from the~~ first computer, wherein the additional individual authentication data unit provides a self certificate including a validity status date and a credential, the self certificate credential being for permitting a second type of access by the first computer to an application provided by the second computer, and wherein the generating includes:

signing the individual authentication data unit by the first computer using a key associated with the public key;

and

c) sending the additional individual authentication data unit by the first computer to the second computer, so that the second computer can~~; and c)~~ verify~~ing~~ authenticity of the additional individual authentication data unit~~, wherein c) includes storing~~ using the first computer's public key that was received from the first computer by the second computer with the basic authentication data. ~~during the certain communication session, and the verifying includes verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key.~~

2. (currently amended) The ~~improved~~ method as claimed in claim 1 wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase.

3. (previously presented) The method as claimed in claim 1, wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

4. (currently amended) The ~~improved~~ method as claimed in claim 1 wherein the second type of access includes an access for an application in which an email message is securely transmitted.

5. (currently amended) The ~~improved~~ method as claimed in claim 1, wherein the authentication data includes an identity certificate, and the method includes:

~~receiving, by the second computer,~~ generating a command from the first computer for the second computer to invalidate a previously presented identity certificate, wherein the previously presented identity certificate includes a validity status date and an identity credential; ~~and~~

~~receiving, by the second computer,~~ generating by the first computer a new identity certificate having a validity status date and an identity credential; and

sending, from the first computer to the second computer, the new identity certificate to replace the invalidated identity certificate, wherein the command to invalidate and the new

identity certificate are both received by the second computer during the certain communication session.

6. (currently amended) A system for providing secure authentication, the system comprising:

means for sending ~~receiving~~ basic authentication data from a first computer to a second computer wherein the basic authentication data provides a certificate including a validity status date and a credential, the credential being for permitting a first type of transaction by the first computer to an application provided by the second computer, ~~for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer;~~ wherein ~~the secure transaction is during a certain communication session between the first and second computer, and~~ the basic authentication data has been certified by an accepted certifying authority, and ~~wherein~~ the basic authentication data sent to the second computer includes a public key of the first computer ~~for permitting a first type of access by the first computer to an application provided by the second computer~~;

~~means for storing a copy of the first computer's public key;~~

~~means for requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer;~~

means for generating ~~receiving the~~ an additional individual authentication data unit by the ~~second computer from~~ the first computer, wherein the additional individual authentication data unit provides a self certificate including a validity status date and a credential, the self certificate credential being for permitting a second type of access by the first computer to an application provided by the second computer, and wherein the means for generating includes:

means for signing the individual authentication data unit by the first computer using a key associated with the public key;

and

means for sending the additional individual authentication data from the first computer to the second computer, so that the second computer can; ~~and means for~~ verifying authenticity of the additional individual authentication data unit, ~~wherein the storing means includes means for~~

~~storing~~ using the first computer's public key that was received from the first computer by the second computer with the basic authentication data, ~~during the certain communication session, and the means for verifying includes means for verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key.~~

7. (previously presented) The system as claimed in claim 6 wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase.

8. (previously presented) The system as claimed in claim 6, wherein the authenticity of said additional individual authentication data is established by means of signature of said accepted certifying authority.

9. (previously presented) The system as claimed in claim 6, wherein the second type of access includes an access for an application in which an email message is securely transmitted.

10. (currently amended) The system as claimed in claim 6, wherein the authentication data includes an identity certificate, and the system includes:

means for ~~receiving, by the second computer,~~ sending a command from the first computer for the second computer to invalidate a previously presented identity certificate, wherein the previously presented identity certificate includes a validity status date and an identity credential; ~~and~~

means for ~~receiving, by the second computer,~~ generating by the first computer a new identity certificate having a validity status date and an identity credential; and

sending, from the first computer to the second computer, the new identity certificate to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session.

11. (currently amended) A computer program product comprising computer readable program code stored on computer readable storage medium embodied therein for providing secure authentication, the computer program product comprising:

computer readable program code ~~means~~ configured for sending ~~receiving~~ basic authentication data from a first computer to a second computer, wherein the basic authentication data provides a certificate including a validity status date and a credential, the credential being for permitting a first type of transaction access by the first computer to an application provided by the second computer~~for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer~~, wherein ~~the secure transaction is during a certain communication session between the first and second computer, and~~ the basic authentication data has been certified by an accepted certifying authority, and ~~wherein~~ the basic authentication data sent to the second computer includes a public key of the first computer ~~for permitting a first type of access by the first computer to an application provided by the second computer;~~

~~computer readable program code means configured for storing a copy of the first computer's public key;~~

~~computer readable program code means configured for requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer;~~

computer readable program code ~~means~~ configured for generating ~~receiving~~ the additional individual authentication data unit by the ~~second computer from the~~ first computer, wherein the additional individual authentication data unit provides a self certificate including a validity status date and a credential, the self certificate credential being for permitting a second type of access by the first computer to an application provided by the second computer, and wherein the computer readable program code configured for generating includes:

computer readable program code configured for signing the individual authentication data unit by the first computer using a key associated with the public key; and

computer readable program code means configured for sending the additional individual authentication data from the first computer to the second computer, so that the second computer can; ~~and computer readable program code means configured for~~ verifying authenticity of the additional individual authentication data unit, ~~wherein the computer readable program code means configured for storing a copy of~~ using the first computer's public key ~~includes computer readable program code means configured for storing the first computer's public key~~ that was received from the first computer with the basic authentication data by the second computer, ~~during the certain communication session, and the verifying includes verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key.~~

12. (previously presented) The computer program product as claimed in claim 11, wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase.

13. (previously presented) The computer program product as claimed in claim 11, wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

14. (previously presented) The computer program product as claimed in claim 11, wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase.

15. (currently amended) The computer program product as claimed in claim 11, wherein the authentication data includes an identity certificate, and the computer program product includes:

computer readable program code ~~means~~ configured for ~~receiving, by the second computer,~~ generating a command from the first computer for the second computer to invalidate a previously presented identity certificate, wherein the previously presented identity certificate includes a validity status date and an identity credential; and

computer readable program code ~~means~~ configured for ~~receiving, by the second computer,~~ generating a new identity certificate having a validity status date and an identity credential; and

computer readable program code configured for sending from the first computer to the second computer, the new identity certificate to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session.